



**Universidad Nacional Abierta y a Distancia
Diplomado de profundización CISCO**

Solución de estudios de caso bajo el uso de tecnología CISCO.

Willian Garcerant, cc 72051758

Cead: *Barranquilla*

Tutor: Diego Edinson Ramírez

Fecha: *Diciembre 9 de 2018*

Tabla de contenido

Introducción	4
Descripción de la prueba	5
Lineamientos para la elaboración del informe	5
Descripción de escenarios propuestos para la prueba de habilidades 1 y 2	7
Desarrollo de escenario 1	7
Configuración inicial de interfaces ISP.....	11
Configuración inicial y de interfaces R1	12
Configuración inicial de interfaces R2.....	13
Configuración inicial de interfaces R3.....	13
Configuración inicial de interfaces SWITCH1	14
Configuración inicial de interfaces SWITCH2	15
Configurar servidores DHCP.....	17
Configuramos una ruta predeterminada desde R1 hasta ISP	17
Configurar Nat en R1	18
Verificamos conectividad	19
Configuramos R3 como DHCPV6 server con (dual-stack)	30
Ping entre equipos de red R3	32
Configuración de rip en cada router.....	34
Descripción de escenario2.....	38
Desarrollo de escenario 2	40
Tabla de direccionamiento.....	41
Configuración de equipos	42
Configuración inicial y de interfaces en R1	45
Configuración inicial y de interfaces en R2	46
Configuración inicial y de interfaces en R3.....	47
Configuración inicial en S1	48
Configuración inicial en S3	49
Configurar OSPFv2 en R1	49
Configurar OSPFv2 en R2	50
Configurar OSPFv2 en R3.....	51
Configurar vlan e interfaces en S1.....	55
Configurar vlan e interfaces en S3.....	56
Configurar vlan y sub-interfaces en R1	57
Asignar ip S1.....	57
Asignar ip S3.....	58
Desactivar interfaces S1	58
Desactivar interfaces S3	58
Configuramos R2 con NAT	59
Configuración de listas de acceso	60
Configuración de listas de acceso	60



Verificar procesos de comunicación	61
Conclusiones	63
Referencias bibliográficas	64

Introducción.

Durante el desarrollo de este diplomado de profundización se realizaron muchas, prácticas y se estudiaron nuevos conceptos que nos permitieron aprender las diferentes configuraciones que se pueden implementar en la puesta en marcha de redes convergentes, algunas de estas configuraciones son críticas y de mucha precisión, por ello se deben realizar prácticas y simulaciones que permitan dominar este tipo de comandos antes de aplicarlos a redes de producción, algunas de estas soluciones son las ACL (Access Control List), otras de menor complejidad como la configuración básica e inicial de equipos como lo es la configuración de contraseñas, encriptación de las mismas, desactivación de interfaces que estén sin utilizar, banner de advertencia a accesos no autorizados, durante este trabajo también se realizó la utilización de comandos de diagnósticos y verificación de configuraciones PING, TRACEROUTE, SHOW IP ROUTE, se realiza la implementación de protocolos importantes para el funcionamiento de las redes, como son algunos de los más utilizados DHCP, NAT, RIPV2, OSPF etc. Se realizaron prácticas de configuraciones ipv4 e ipv6 mediante DHCPV6 y (dual-stack). Otra de las implementaciones básicas e importantes fue la del concepto de VLAN, siendo estas importantes para la configuración y enrutamiento del tráfico de red, que permita de forma estructurada la segmentación de redes, permite mejorar el rendimiento y facilita administración de la red.

Solución de estudios de caso bajo el uso de tecnología CISCO.

Descripción general de la prueba de habilidades

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los **dos (2) escenarios propuestos**, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos **ping, traceroute, show ip route, entre otros**.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: **Packet Tracer** o **GNS3**.

- Es muy importante mencionar que esta actividad es de carácter **INDIVIDUAL y OBLIGATORIA**.
- Toda evidencia de **copy-paste o plagio (de la web o de otros informes)** será penalizada con severidad.

Lineamientos para la elaboración del Informe

Finalmente, el informe a presentar deberá cumplir con las normas **ICONTEC 1486** para la presentación de trabajos escritos e incluir los siguientes elementos en su contenido:

- **Portada**
- **Tabla de contenido**
- **Introducción**
- **Desarrollo de los dos escenarios**

IMPORTANTE: Para cada uno de los escenarios se debe describir el paso a paso de cada punto realizado y deben digitar el código de configuración aplicado (no incluir imágenes ni capturas de pantalla). Las imágenes o

capturas de pantalla sólo serán usadas para evidenciar los resultados de comandos como **ping, traceroute, show ip route, entre otros.**

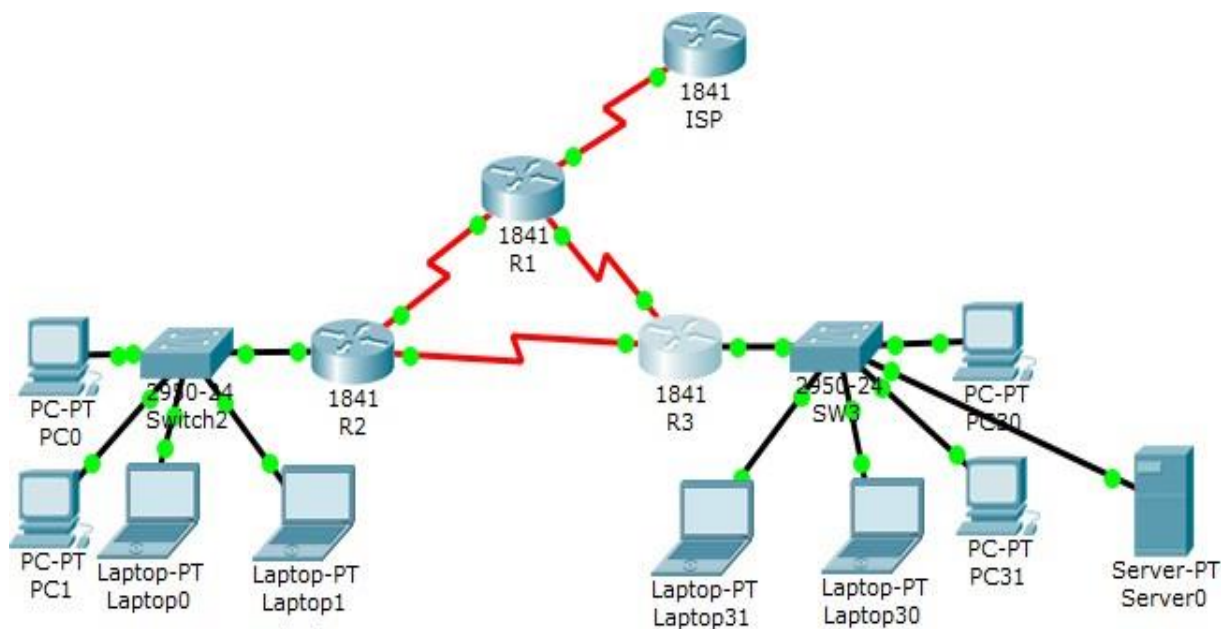
- **Conclusiones**
- **Referencias Bibliográficas**

El informe deberá estar acompañado de las respectivas evidencias de configuración de los dispositivos (Packet Tracer ó GNS3), las cuales generarán veracidad al trabajo realizado. **El informe deberá ser entregado en el espacio creado para tal fin en el Campus Virtual de la UNAD.**

IMPORTANTE: Teniendo en cuenta que este documento deberá ser entregado al final del curso en el Repositorio Institucional, acorde con los lineamientos institucionales para grado. El procedimiento será socializado al finalizar el curso.

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1



Topología de red.

El administrador	Interfases	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	Se0/1/0	10.0.0.1	255.255.255.252	N/D
	Se0/1/1	10.0.0.5	255.255.255.252	N/D
R2	Fa0/0,100	192.168.20.1	255.255.255.0	N/D
	Fa0/0,200	192.168.21.1	255.255.255.0	N/D

R3	Se0/0/0	10.0.0.2	255.255.255.252	N/D
	Se0/0/1	10.0.0.9	255.255.255.252	N/D
	Fa0/0	192.168.30.1	255.255.255.0	N/D
		2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

Tabla de direccionamiento

PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP
PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Tabla de asignación de VLAN y de puertos

Dispositivo	VLAN	Nombre	Interfaz
SW2	100	LAPTOPS	Fa0/2-3
SW2	200	DESTOPS	Fa0/4-5
SW3	1	-	Todas las interfaces

Tabla de enlaces troncales

Dispositivo local	Interfaz local	Dispositivo remoto
SW2	Fa0/2-3	100

Situación

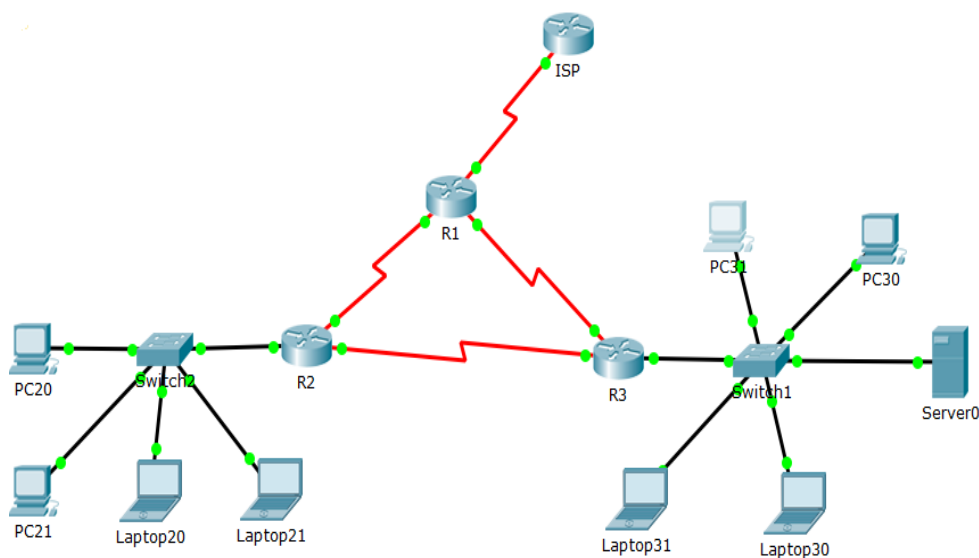
En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente.

Descripción de las actividades

- **SW1** VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.
- Los puertos de red que no se utilizan se deben deshabilitar.
- **La información** de dirección **IP R1, R2 y R3** debe cumplir con la tabla 1.
- **Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31** deben obtener información IPv4 del servidor DHCP.
- **R1** debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se **llama INSIDE-DEVS**.
- **R1** debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en **el dominio** RIPV2.

- **R2** es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.
- **R2** debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.
- El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).
- La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.
- La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).
- R1, R2 y R3 intercambian información de routing mediante RIP versión 2.
- R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.
- Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo **el R3** deberían poder hacer IPv6-ping entre ellos y el servidor.

Desarrollo de escenario 1.



1.1 Configuración inicial y de interfaces.

ISP.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#
ISP(config)#end
ISP#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#
%SYS-5-CONFIG_I: Configured from console by console

ISP#
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#no ip domain-lookup
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#pass cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 4
ISP(config-line)#pass cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption
ISP(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado #
ISP(config)#int s0/0/0
ISP(config-if)#ip address 200.123.211.1 255.255.255.0
ISP(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
ISP(config-if)#do wr
Building configuration...
[OK]
```

***Configuración inicial ISP con los parámetros básicos.

Configuración inicial y de interfaces R1.

```
R1>ena
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado #
R1(config)#int s0/0/0
R1(config-if)#ip address 200.123.211.2 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
R1(config-if)#int s0/1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
R1(config-if)#int s0/1/1
R1(config-if)#ip address 10.0.0.5 255.255.255.252
R1(config-if)#no shut
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
R1(config-if)#do wr
Building configuration...
[OK]
***Configuración inicial R1 con los parámetros básicos.
```

Configuración inicial y de interfaces R2.

```
R2>ena
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado #
R2(config)#int s0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if) #no shut
R2(config-if) #
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
R2(config-if) #int s0/0/1
R2(config-if) #ip address 10.0.0.9 255.255.255.252
R2(config-if) #no shut
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R2(config-if) #do wr
Building configuration...
[OK]
***Configuración inicial R2 con los parámetros básicos.
```

Configuración inicial y de interfaces R3.

```
R3>ena
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#no ip domain-lookup
```

```
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line) #pass cisco
R3(config-line) #login
R3(config-line) #line vty 0 4
R3(config-line) #pass cisco
R3(config-line) #login
R3(config-line) #exit
R3(config)#service password-encryption
R3(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado #
R3(config)#int s0/0/0
R3(config-if) #ip address 10.0.0.6 255.255.255.252
R3(config-if) #no shut
R3(config-if) #
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
R3(config-if) #int s0/0/1
R3(config-if) #ip address 10.0.0.10 255.255.255.252
R3(config-if) #no shut
R3(config-if) #
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state
to up
R3(config-if) #do wr
Building configuration...
[OK]
R3(config-if) #
```

***Configuración inicial R3 con los parámetros básicos.

Configuración inicial y de interfaces Switch1.

```
Switch>ena
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#enable secret class
Switch(config)#line console 0
Switch(config-line) #pass cisco
```

```
Switch(config-line) #login
Switch(config-line) #exit
Switch(config)#service password-encryption
Switch(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido acceso no Autorizado #
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#hostname switch1
switch1(config)#
```

***Configuración inicial switch1 con los parámetros básicos.

Configuración inicial y de interfaces Switch2.

```
Switch2#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#no ip domain-lookup
Switch2(config)#enable secret class
Switch2(config)#line console 0
Switch2(config-line) #pass cisco
Switch2(config-line) #login
Switch2(config-line) #line vty 0 4
Switch2(config-line) #pass cisco
Switch2(config-line) #login
Switch2(config-line) #exit
Switch2(config)#service password-encryption
Switch2(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido acceso no Autorizado #
Switch2(config)#do wr
Building configuration...
[OK]
Switch2(config)#
```

***Configuración inicial switch2 con los parámetros básicos.

1.2 Configurar vlan y puertos en acceso y troncales.

R2.

```
R2(config)#int f0/0
```

```
R2(config-if) #no shut
R2(config-if) #
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R2(config-if) #int f0/0.100
R2(config-subif) #
%LINK-5-CHANGED: Interface FastEthernet0/0.100, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.100,
changed state to up
R2(config-subif) #encapsulation dot1 100
R2(config-subif) #ip address 192.168.20.1 255.255.255.0
R2(config-subif) #int f0/0.200
R2(config-subif) #
%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200,
changed state to up
R2(config-subif) #ip address 192.168.21.1 255.255.255.0
% Configuring IP routing on a LAN subinterface is only allowed if that
subinterface is already configured as part of an IEEE 802.10, IEEE 802.1Q,
or ISL vlan.
R2(config-subif) #encapsulation dot1q 200
R2(config-subif) #ip address 192.168.21.1 255.255.255.0
R2(config-subif) #do wr
Building configuration...
[OK]
```

*** Configuración de vlan en R2, 100 y 200 para conexión LAN.

```
Switch2.
Switch2(config)#
Switch2(config)#vlan 100
Switch2(config-vlan)#name LABTOPS
Switch2(config-vlan)#vlan 200
Switch2(config-vlan)#name DESKTOPS
Switch2(config-vlan)#EXIT
Switch2(config)#do wr
Building configuration...
[OK]
Switch2(config)#int f0/1
Switch2(config-if)#switchport mode trunk
```

```
Switch2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to down
```


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

```
Switch2(config-if)#switchport trunk native vlan 1
```

```
Switch2(config-if)#int f0/2
```

```
Switch2(config-if)#switch mode access
```

```
Switch2(config-if)#switch access vlan 100
```

```
Switch2(config-if)#int f0/3
```

```
Switch2(config-if)#switch mode access
```

```
Switch2(config-if)#switch access vlan 100
```

```
Switch2(config-if)#int f0/4
```

```
Switch2(config-if)#switch mode access
```

```
Switch2(config-if)#switch access vlan 200
```

```
Switch2(config-if)#int f0/5
```

```
Switch2(config-if)#switch mode access
```

```
Switch2(config-if)#switch access vlan 200
```

*** Configuración de interfaces con vlan 100 y 200 en modo acceso.

Configurar servidores DHCP.

R2.

```
R2#config t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)#ip dhcp pool DESKTOP
```

```
R2(dhcp-config)#dns-server 8.8.8.8
```

```
R2(dhcp-config)#network 192.168.21.0 255.255.255.0
```

```
R2(dhcp-config)#default-router 192.168.21.1
```

```
R2(dhcp-config)#ip dhcp pool LABTOP
```

```
R2(dhcp-config)#dns-server 8.8.8.8
```

```
R2(dhcp-config)#default-router 192.168.20.1
```

```
R2(dhcp-config)#network 192.168.20.0 255.255.255.0
```

```
R2(dhcp-config)#do wr
```

Building configuration...

[OK]

```
R2(dhcp-config)#
```

*** Configuración de servidores Dhcp de vlan 100 y 200.

Configuramos una ruta predeterminada desde R1 hasta ISP.

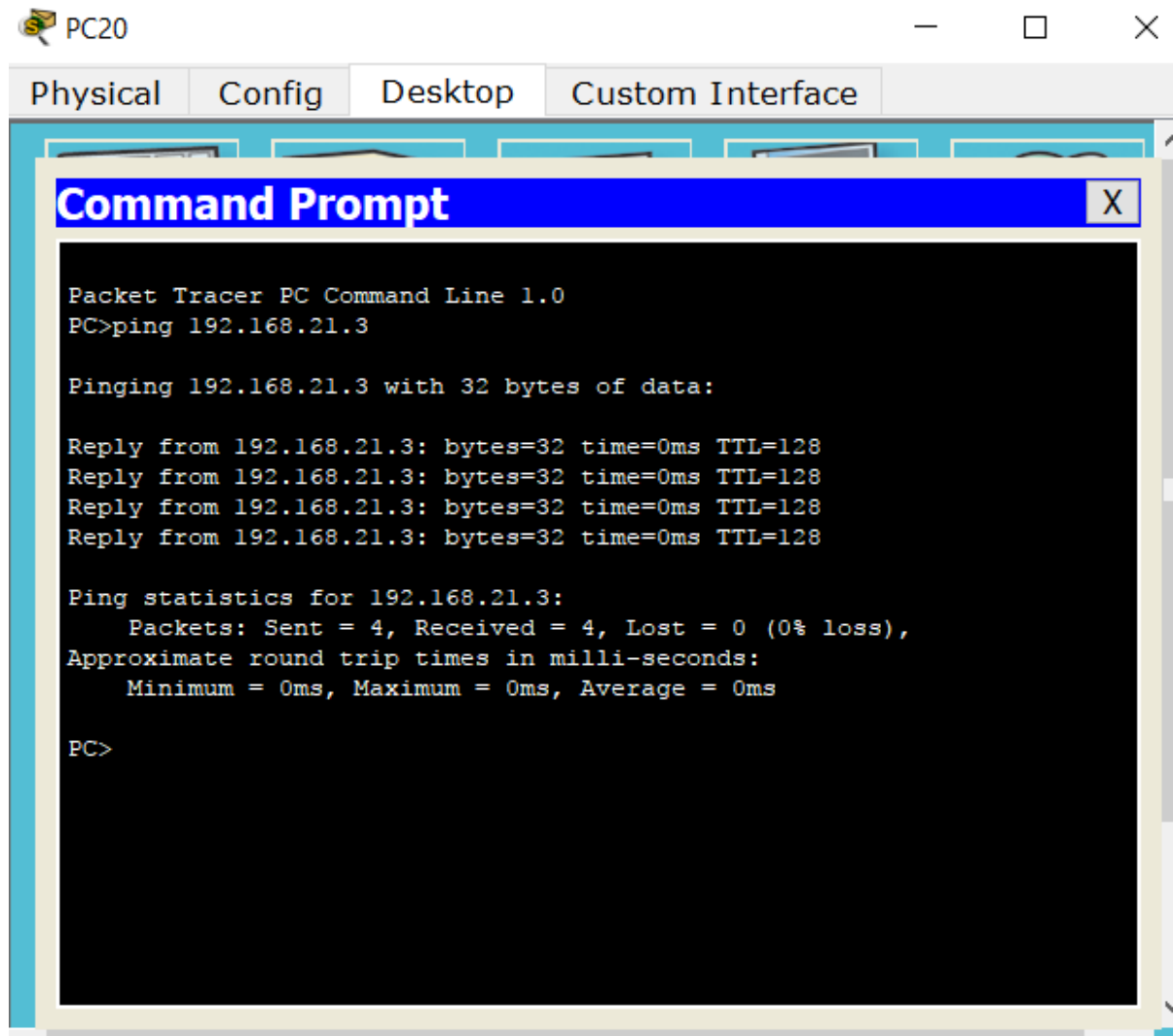
```
R1(config)#ip route 0.0.0.0 0.0.0.0 200.123.211.1
```

Configurar Nat en R1.

```
R1>ena
Password:
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip access-list standard INSIDE-DEVS
R1(config-std-nacl)#remark ACL CLIENTES
R1(config-std-nacl)#permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)#permit 192.168.21.0 0.0.0.255
R1(config-std-nacl)#permit 10.0.0.0 0.0.0.255
R1(config-std-nacl)#permit 192.168.30.0 0.0.0.255
R1(config-std-nacl)#exit
R1(config)#ip nat pool public-access 200.123.211.1 200.123.211.254 netmask
255.255.255.0
R1(config)#ip nat inside source list INSIDE-DEVS pool public-access overload
R1(config)#int s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#int s0/0/0
R1(config-if)#ip nat outside
R1(config)#int s0/1/1
R1(config-if)#ip nat inside
R1(config-if)#do wr
Building configuration...
[OK]
```


Verificamos conectividad.

Ping PC20 a PC21.



Ping desde el Pc-20 al Pc-21 donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping PC20 a LAPTOP20

 PC20

Physical
Config
Desktop
Custom Interface

Command Prompt

```

PC>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.3: bytes=32 time=0ms TTL=127
Reply from 192.168.20.3: bytes=32 time=4ms TTL=127
Reply from 192.168.20.3: bytes=32 time=1ms TTL=127


Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

PC>

```

Ping desde el Pc-20 al Laptop-20 donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping PC20 a LAPTOP21

 PC20

Physical
Config
Desktop
Custom Interface

Command Prompt

```

PC>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=0ms TTL=127
Reply from 192.168.20.2: bytes=32 time=0ms TTL=127
Reply from 192.168.20.2: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

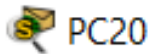
PC>

```

Ping desde el Pc-20 al Laptop-21 donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping a ISP.

Ping PC20 a ISP.



Physical Config Desktop Custom Interface

Command Prompt

```
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

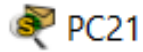
Reply from 200.123.211.1: bytes=32 time=10ms TTL=253
Reply from 200.123.211.1: bytes=32 time=7ms TTL=253
Reply from 200.123.211.1: bytes=32 time=6ms TTL=253
Reply from 200.123.211.1: bytes=32 time=9ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 10ms, Average = 8ms

PC>
```

Ping desde el Pc-20 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping PC21 a ISP.



Physical Config Desktop Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=3ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=8ms TTL=253
Reply from 200.123.211.1: bytes=32 time=7ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 8ms, Average = 5ms

PC>|
```

Ping desde el Pc-21 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping LAPTOP20 a ISP.



Laptop20

Physical Config Desktop Custom Interface

Command Prompt

```
Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

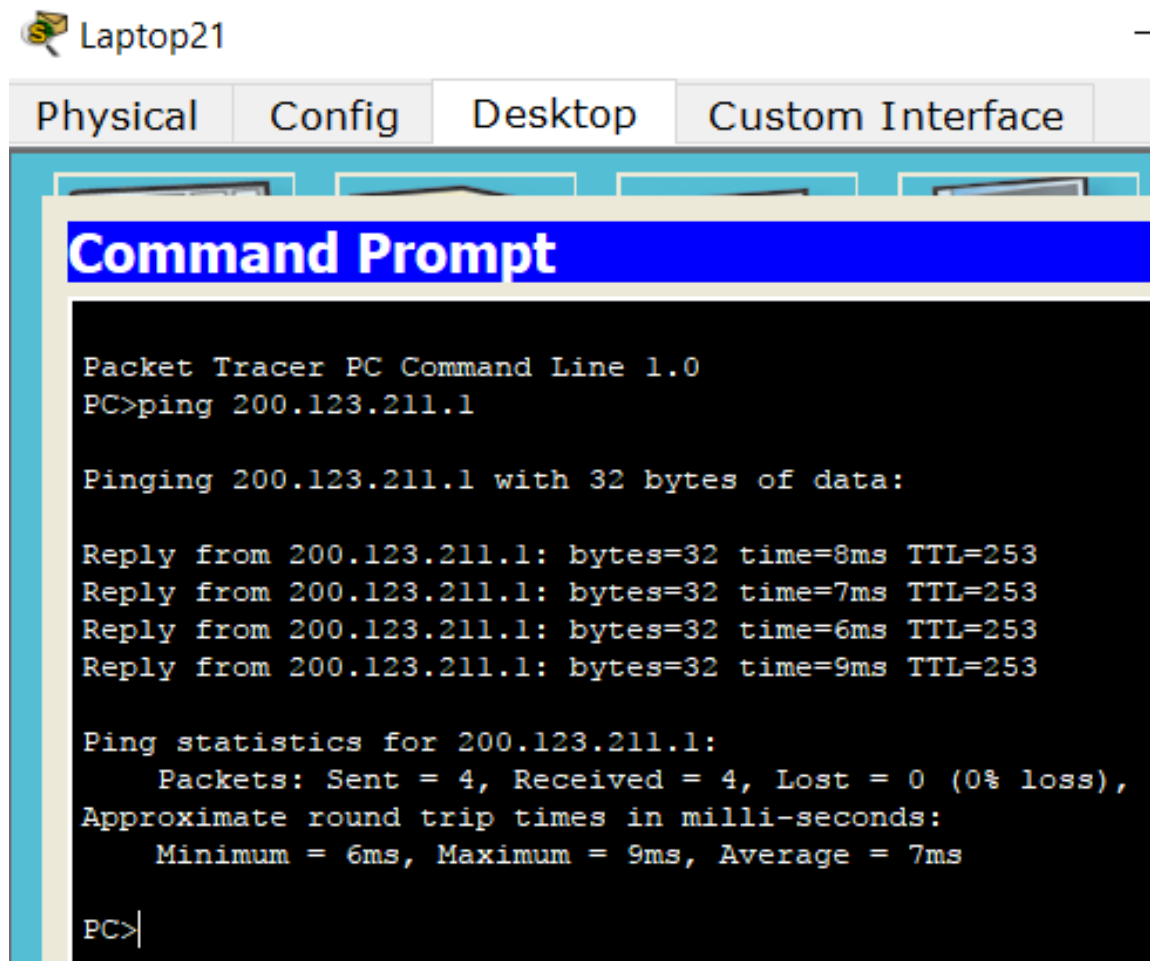
Reply from 200.123.211.1: bytes=32 time=9ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=4ms TTL=253
Reply from 200.123.211.1: bytes=32 time=7ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 5ms

PC>
```


Ping desde el Laptop-20 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping LAPTOP21 a ISP.



Ping desde el Laptop-21 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping PC31 a ISP.

 PC31

Physical
Config
Desktop
Custom Interface

Command Prompt

```

Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253


Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

PC>|

```

Ping desde el Pc-31 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping PC30 a ISP

 PC30

Physical
Config
Desktop
Custom Interface

Command Prompt

```

Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=6ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253


Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 6ms, Average = 3ms

PC>

```

Ping desde el Pc-30 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping Server0 a ISP.

 Server0

Physical
Config
Services
Desktop
Custom Int

Command Prompt

```

Packet Tracer SERVER Command Line 1.0
SERVER>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=10ms TTL=253
Reply from 200.123.211.1: bytes=32 time=7ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 10ms, Average = 5ms

SERVER>

```

Ping desde el Server0 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping LAPTOP31 a ISP.



Laptop31

Physical
Config
Desktop
Custom Interface

Command Prompt

```

Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=9ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=9ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 5ms

PC>

```

Ping desde el Laptop-31 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping LAPTOP30 a ISP.



Laptop30

Physical
Config
Desktop
Custom Interface

Command Prompt

```

Packet Tracer PC Command Line 1.0
PC>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=6ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=7ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 7ms, Average = 4ms

PC>

```

Ping desde el Laptop-30 al ISP donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Configuramos R3 como DHCPV6 server con (dual-stack).

```

R3>ena
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#int f0/0
R3(config-if)#ip address 192.168.30.1 255.255.255.0

```

```
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#ipv6 dhcp server vlan_1
R3(config-if)#ipv6 nd other-config-flag
R3(config-if)#no shut
```

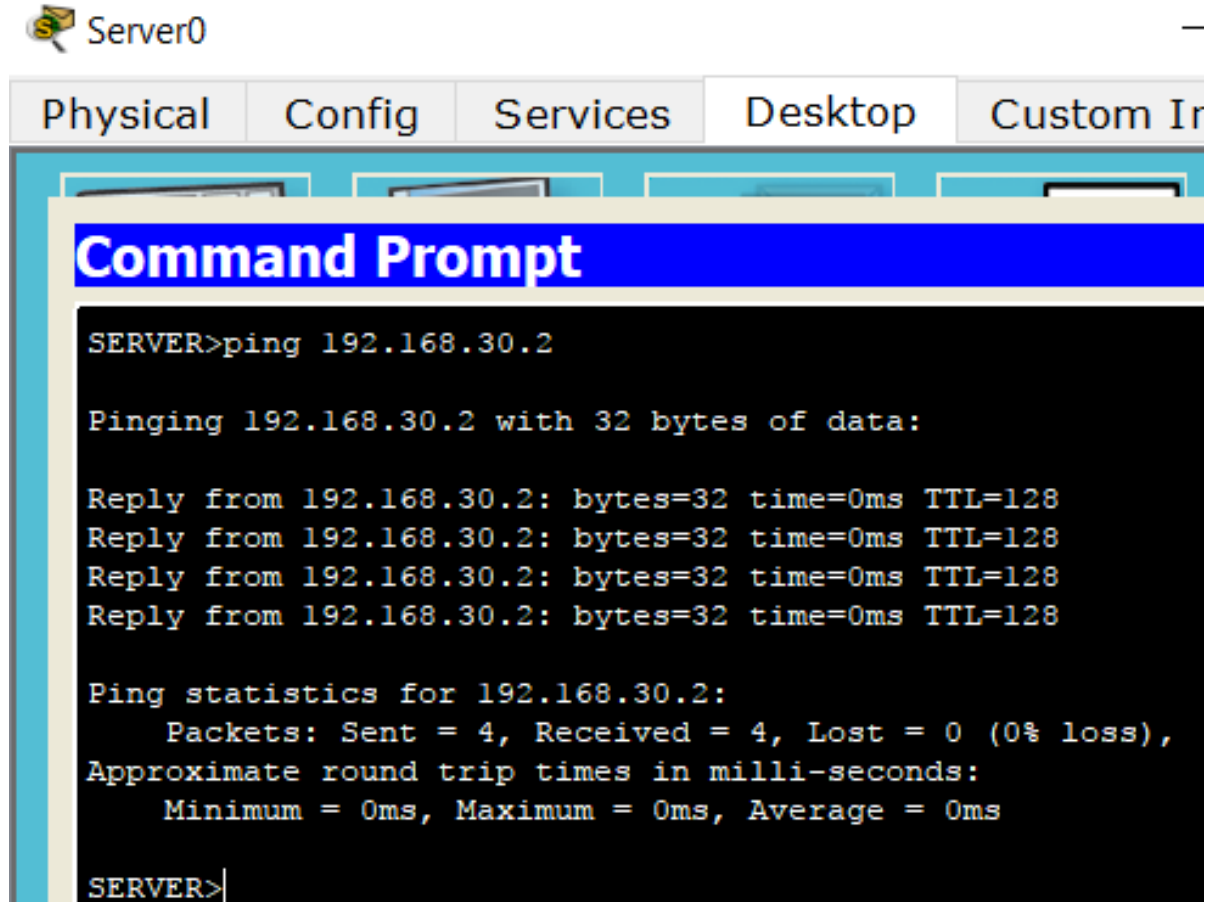
```
R3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
```

```
R3(config-if)#ip dhcp pool vlan_1
R3(dhcp-config)#network 192.168.30.1 255.255.255.0
R3(dhcp-config)#default-router 192.168.30.1
R3(dhcp-config)#ipv6 dhcp pool vlan_1
R3(config-dhcp)#dns-server 2001:db8:130::
R3(config-dhcp)#exit
R3(config)#do wr
Building configuration...
[OK]
R3(config)#
```

Ping entre equipos de red R3.

Ping SERVER0 a LAPTOP31.



Server0

Physical Config Services Desktop Custom Ir

Command Prompt

```
SERVER>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.30.2: bytes=32 time=0ms TTL=128
Reply from 192.168.30.2: bytes=32 time=0ms TTL=128
Reply from 192.168.30.2: bytes=32 time=0ms TTL=128
Reply from 192.168.30.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

SERVER>
```

Ping desde el Server0 al Laptop-31 donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping LAPTOP30 a PC31.



Laptop30

Physical
Config
Desktop
Custom Interface

Command Prompt

```

PC>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=0ms TTL=128
Reply from 192.168.30.3: bytes=32 time=0ms TTL=128
Reply from 192.168.30.3: bytes=32 time=0ms TTL=128
Reply from 192.168.30.3: bytes=32 time=0ms TTL=128


Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

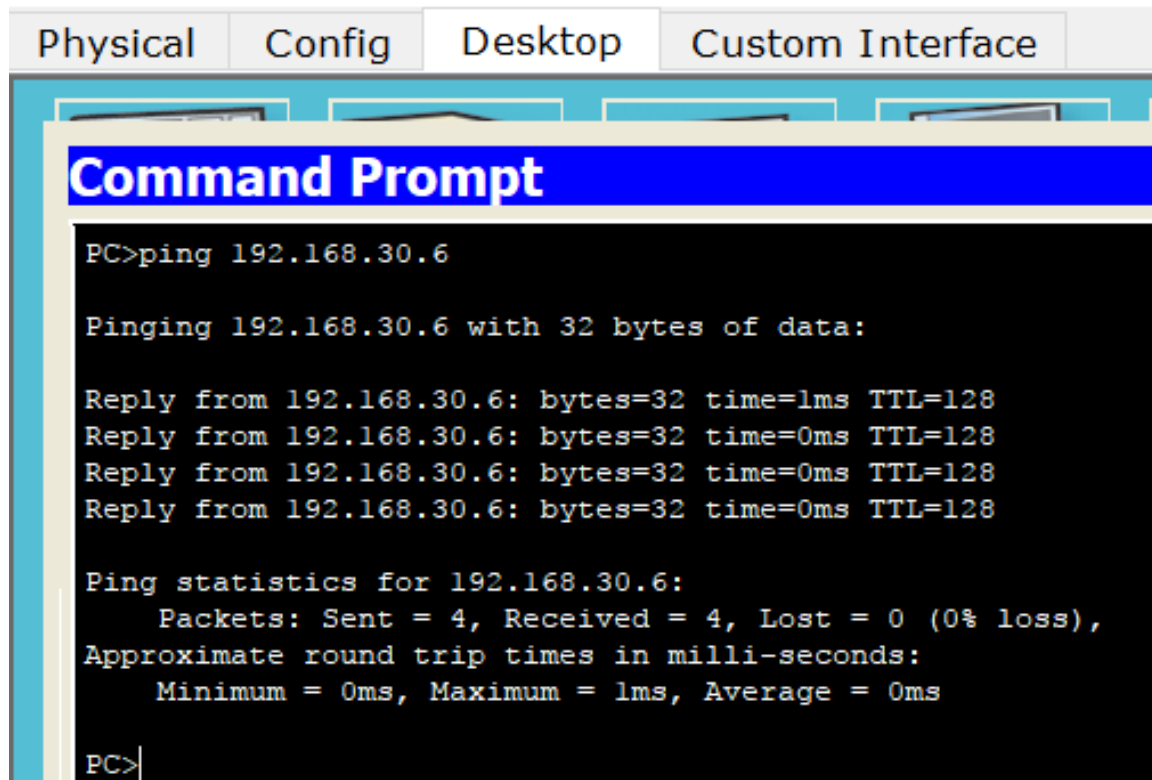
PC>

```

Ping desde el Laptop-30 al Pc-31 donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Ping PC31 a PC30.

 PC31



Ping desde el Pc-31 al Pc-30 donde se evidencia una respuesta de conectividad protocolo ICMP correcta.

Configuración de rip en cada router.

R2.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.30.0
R2(config-router)#network 192.168.20.0
R2(config-router)#network 192.168.21.0
R2(config-router)#network 10.0.0.0
```

```

R2(config-router)#network 10.0.0.8
R2(config-router)#
R2>ena
Password:
R2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 25 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0.100  2      2
  FastEthernet0/0.200  2      2
  Serial0/0/1          2      2
  Serial0/0/0          2      2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
  192.168.20.0
  192.168.21.0
  192.168.30.0
Passive Interface(s):
Routing Information Sources:
  Gateway         Distance      Last Update
  10.0.0.1         120           00:00:23
  10.0.0.10        120           00:00:22
Distance: (default is 120)
R2#

```

R1

```

R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#router rip
R1(config-router)#network 10.0.0.4
R1(config-router)#network 10.0.0.0
R1(config-router)#default-information originate
R1(config-router)#do wr
Building configuration...
[OK]

```

R1(config-router)#

```
R1>ena
Password:
R1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 14 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/1/0         2     2
  Serial0/1/1         2     2
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
  10.0.0.0
Passive Interface(s):
Routing Information Sources:
  Gateway            Distance      Last Update
  10.0.0.2            120          00:00:20
  10.0.0.6            120          00:00:10
Distance: (default is 120)
R1#
```

R3

```
R3>ena
Password:
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.30.0
R3(config-router)#network 10.0.0.8
R3(config-router)#network 10.0.0.4
R3(config-router)#do wr
```



R3

Physical

Config

CLI

IOS Command Line Interface

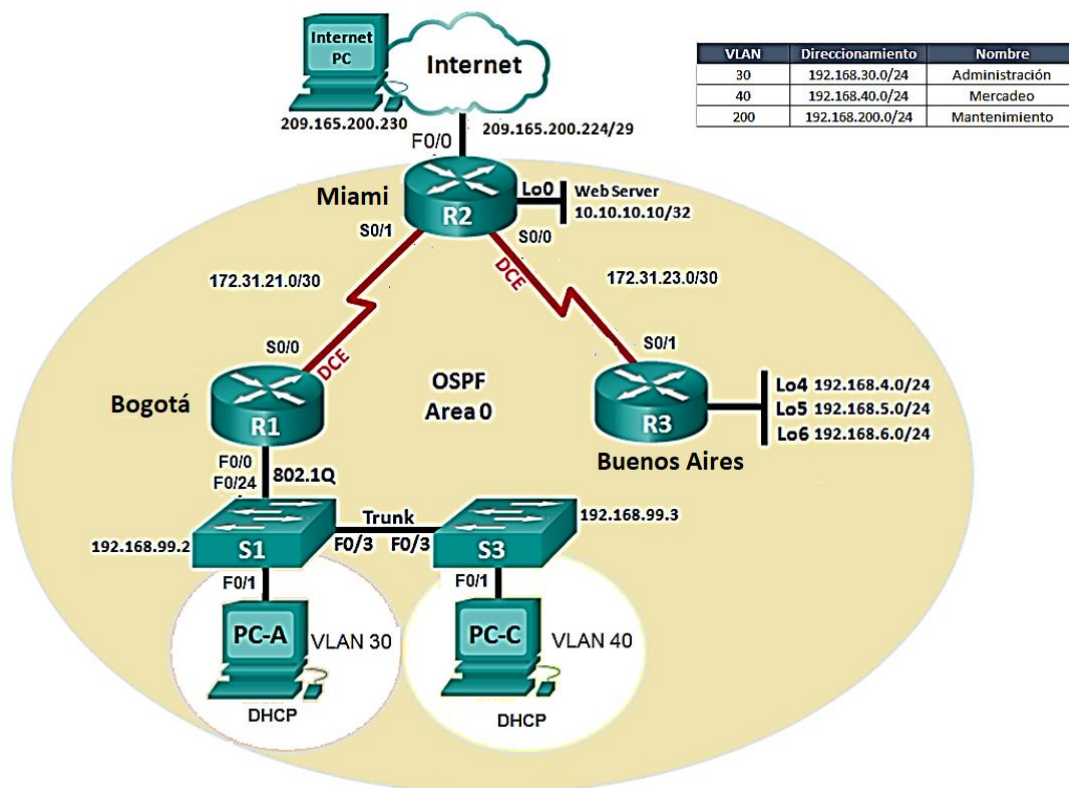
```

Password:
R3#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive 2
    Interface          Send  Recv  Triggered RIP  Key-chain
  FastEthernet0/0      2      2
  Serial10/0/1         2      2
  Serial10/0/0         2      2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    10.0.0.0
    192.168.30.0
  Passive Interface(s):
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.0.0.5         120           00:00:16
    10.0.0.9         120           00:00:13
  Distance: (default is 120)
R3#

```

Escenario 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.



1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario
2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1

Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
 - Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
 - Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.
3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.
 4. En el Switch 3 deshabilitar DNS lookup
 5. Asignar direcciones IP a los Switches acorde a los lineamientos.
 6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
 7. Implement DHCP and NAT for IPv4
 8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
 9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

10. Configurar NAT en R2 para permitir que los hosts puedan salir a internet
11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Desarrollo de Escenario 2.

- 2.1 Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.

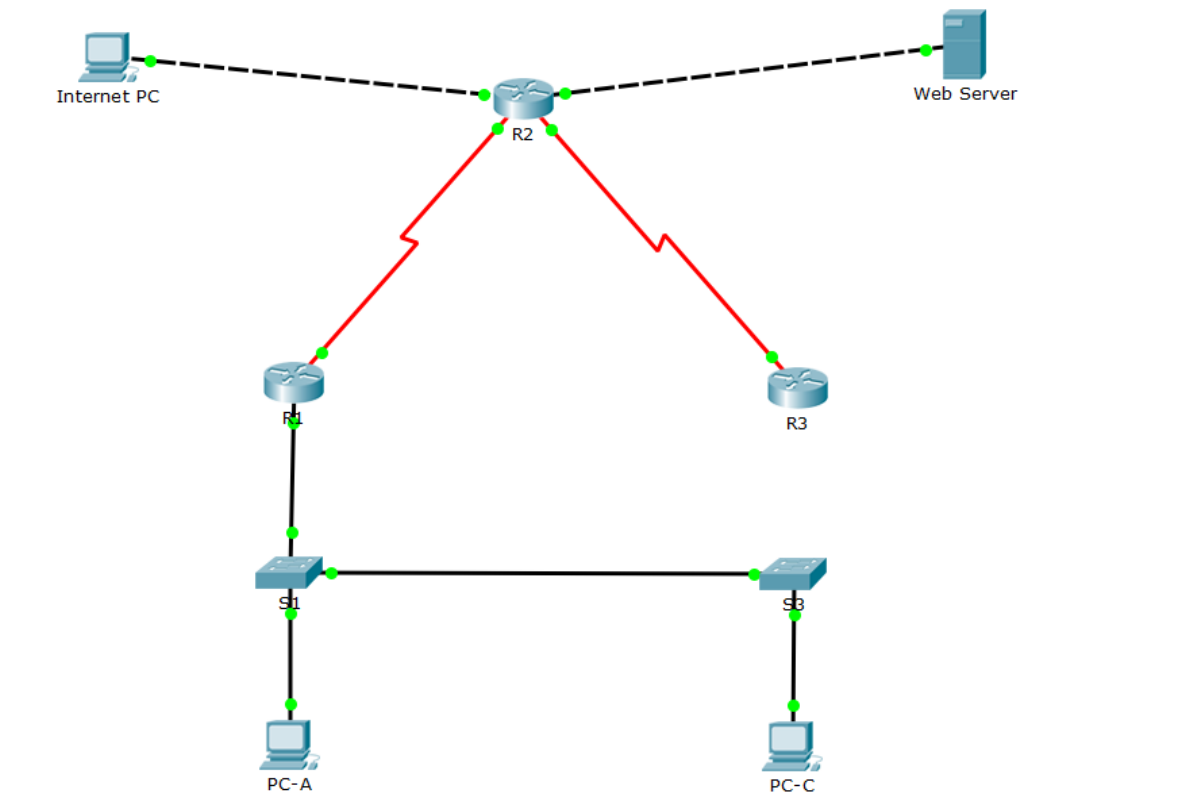


Tabla de direccionamiento.

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado	Observaciones
R1	S0/1/0 (DCE)	172.31.21.1	255.255.255.252	N/A	
	G0/0	N/A	N/A	N/A	802.1Q
R2	S0/1/1 (DCE)	172.31.21.2	255.255.255.252	N/A	
	S0/1/0 (DCE)	172.31.23.1	255.255.255.252	N/A	
	G0/0	209.165.200.225	255.255.255.248	N/A	
	G0/1	10.10.10.1	255.255.255.0	N/A	
R3	S0/1/0 (DCE)	172.31.23.2	255.255.255.252	N/A	
	Lo4	192.168.4.1	255.255.255.0	N/A	
	Lo5	192.168.5.1	255.255.255.0	N/A	
	Lo6	192.168.6.1	255.255.255.0	N/A	
Internet-PC	NIC	209.165.200.230	255.255.255.248	209.165.200.225	
PC-A	NIC	DHCP	DHCP	DHCP	
PC-C	NIC	DHCP	DHCP	DHCP	
WEB SERVER	NIC	10.10.10.10	255.255.255.0	10.10.10.1	
S1	VLAN 200	192.168.99.2	255.255.255.0	192.168.99.1	
	F0/3	N/A	N/A	N/A	802.1Q

	F0/24	N/A	N/A	N/A	802.1Q
S3	VLAN 200	192.168.99.3	255.255.255.0	192.168.99.1	
	F0/3	N/A	N/A	N/A	802.1Q

Configuración de equipos.

PC-A

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☒ DHCP ☐ Static Requesting IP Address

IP Address

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

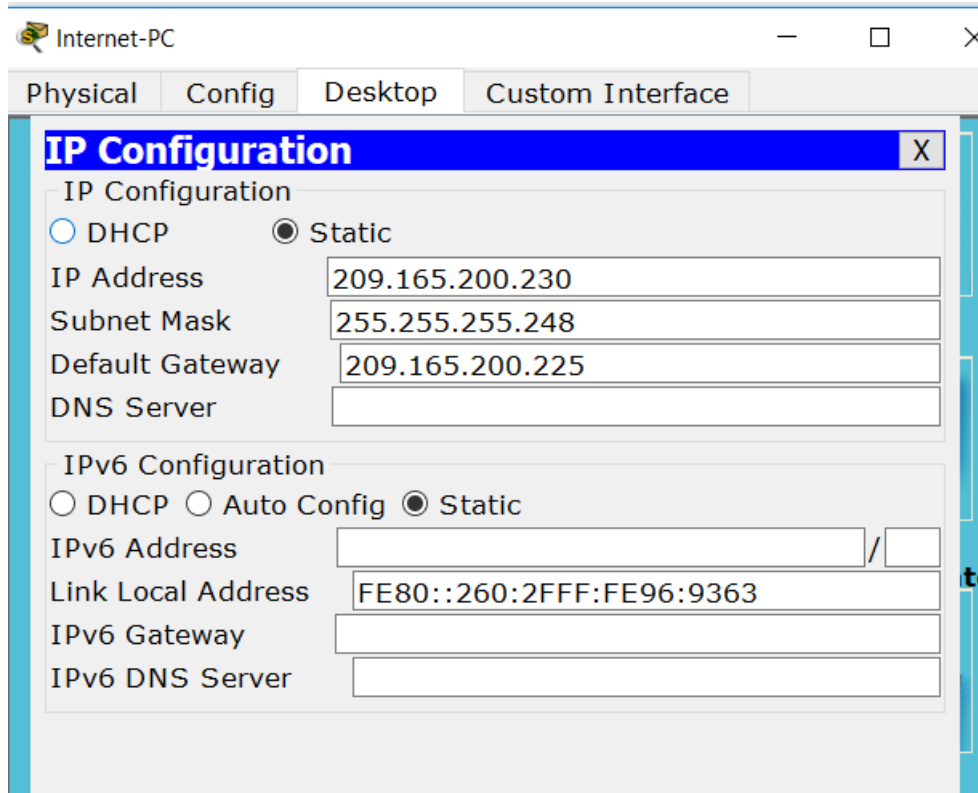
IPv6 Address

Link Local Address FE80::2D0:97FF:FEEE:C724

IPv6 Gateway

IPv6 DNS Server

Los equipos deben estar en Dhcp, según lo indica la guía.



The screenshot shows a web-based configuration interface for an "Internet-PC". The interface has four tabs: "Physical", "Config", "Desktop", and "Custom Interface". The "Config" tab is active, and a sub-tab titled "IP Configuration" is selected, indicated by a blue header bar with a close button (X). Below the header, there are two main sections: "IP Configuration" and "IPv6 Configuration".

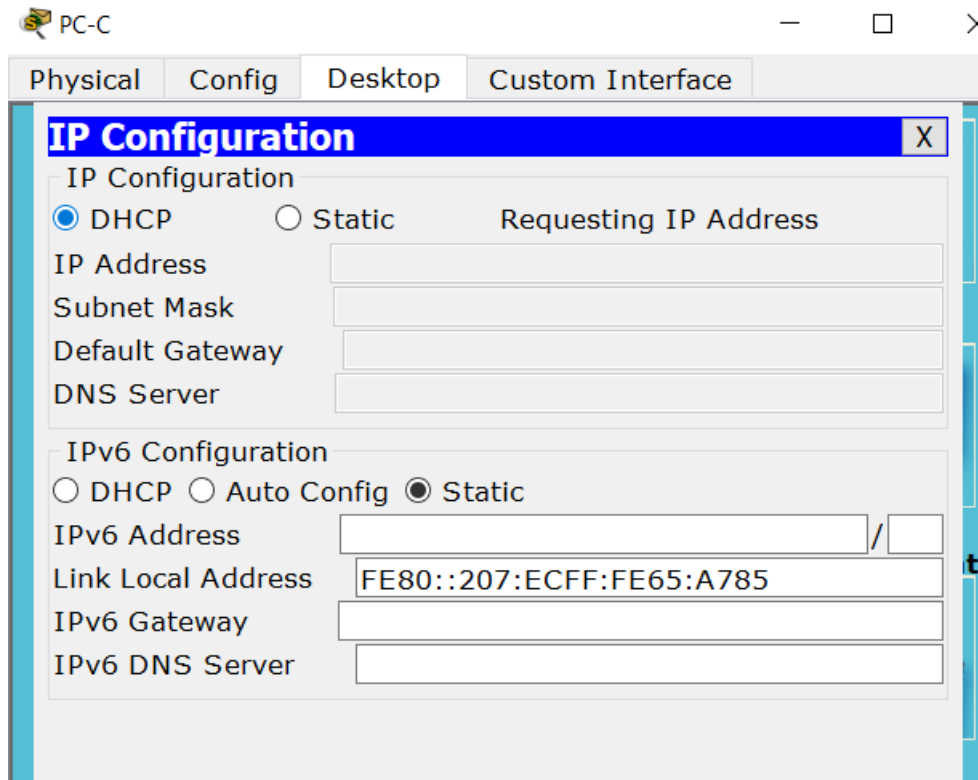
IP Configuration:

- Radio buttons: ☐ DHCP, ☒ Static
- IP Address: 209.165.200.230
- Subnet Mask: 255.255.255.248
- Default Gateway: 209.165.200.225
- DNS Server: (empty field)

IPv6 Configuration:

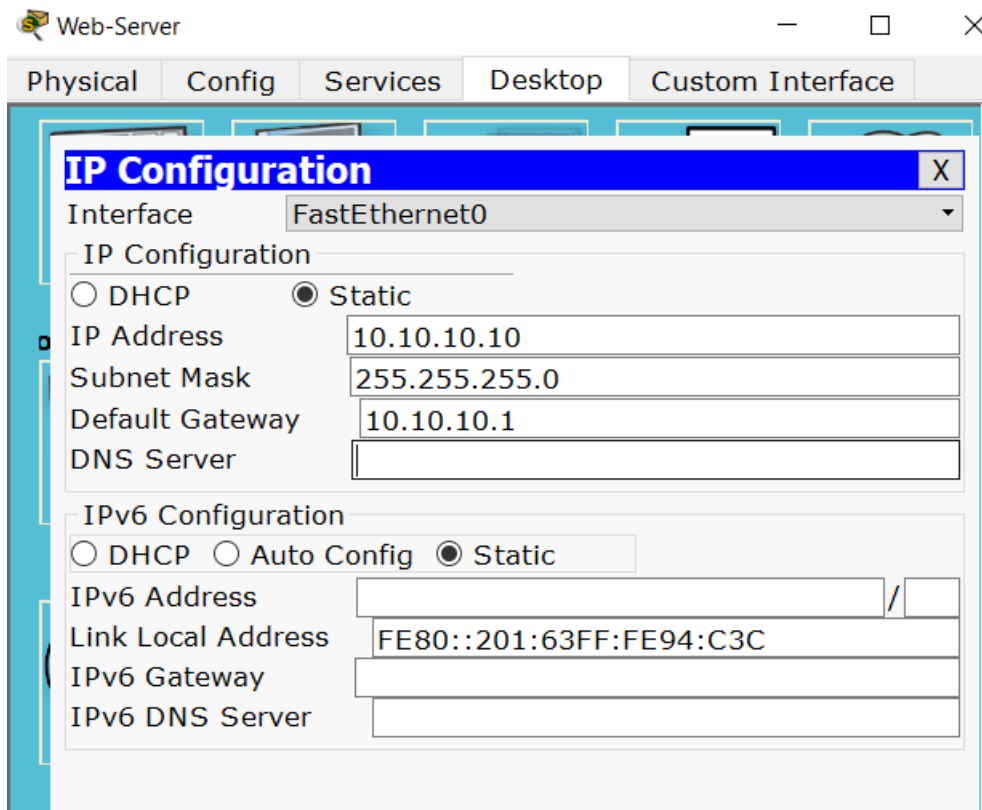
- Radio buttons: ☐ DHCP, ☐ Auto Config, ☒ Static
- IPv6 Address: (empty field) / (empty field)
- Link Local Address: FE80::260:2FFF:FE96:9363
- IPv6 Gateway: (empty field)
- IPv6 DNS Server: (empty field)

Este equipo deben estar en conexión estatica con las ip especificadas, para lograr una correcta conexión y funcionamiento, según lo indica la guía.



The screenshot shows a window titled "PC-C" with a tabbed interface. The "Config" tab is selected, and the "IP Configuration" sub-tab is active. The "IP Configuration" section has two radio buttons: "DHCP" (selected) and "Static". Below these are four text input fields: "IP Address", "Subnet Mask", "Default Gateway", and "DNS Server". The "IPv6 Configuration" section has three radio buttons: "DHCP", "Auto Config", and "Static" (selected). Below these are four text input fields: "IPv6 Address" (with a slash separator), "Link Local Address" (containing the value "FE80::207:ECFF:FE65:A785"), "IPv6 Gateway", and "IPv6 DNS Server".

Estos equipos deben estar en conexión dhcp, para lograr una correcta conexión y funcionamiento, según lo indica la guía.



Web-Server

Physical Config Services Desktop Custom Interface

IP Configuration X

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address: 10.10.10.10

Subnet Mask: 255.255.255.0

Default Gateway: 10.10.10.1

DNS Server:

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::201:63FF:FE94:C3C

IPv6 Gateway:

IPv6 DNS Server:

Estos equipos deben estar en conexión estática con las ip especificadas, para lograr una correcta conexión y funcionamiento, según lo indica la guía

Configuración inicial y de interfaces en R1.

```
R1>ena
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.

```

Prohibido acceso no Autorizado#

```
R1(config)#int s0/1/0
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#no shut
R1(config-if)#clock rate 128000
R1(config-if)#no shut
R1(config-if)#do wr
Building configuration...
[OK]
```

Configuración inicial y de interfaces en R2.

```
R2>ena
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#no ip domain-lookup
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado#
```

```
R2(config)#int s0/0/0
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#int s0/0/1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#int f0/0
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shut
```

```
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
R2(config-if)#int f0/1
R2(config-if)#ip address 10.10.10.1 255.255.255.0
R2(config-if)#no shut
```

```
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
```

```
R2(config-if)#do wr
Building configuration...
[OK]
```

Configuración inicial y de interfaces en R3.

```
R3>ena
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#no ip domain-lookup
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido acceso no Autorizado#
```

```
R3(config)#do wr
Building configuration...
[OK]
R3(config)#int s0/1/0
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#clock rate 128000
R3(config-if)#
R3(config-if)#int Lo 4
```

```
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up

```
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int Lo 5
```

```
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up

```
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int Lo 6
```

```
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
```

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

```
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#no shut
```

Configuración inicial en S1.

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado
#
```

```
S1(config)#do wr
```


Configuración inicial en S3.

```

S3>ena
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #
Enter TEXT message. End with the character '#'.
Prohibido el acceso no Autorizado #

S3(config)#do wr
Building configuration...
[OK]
S3(config)#

```

2.2 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Configurar OSPFv2 en R1.

```

R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0

```

```
R1(config-router)#network 192.168.30.0 0.0.0.3 area 0
R1(config-router)#network 192.168.40.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/0.30
R1(config-router)#passive-interface g0/0.40
R1(config-router)#passive-interface g0/0.200
R1(config-router)#passive-interface g0/0
R1(config-router)#auto-cost reference-bandwidth 9500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#exit
R1(config)#int s0/1/0
R1(config-if)#bandwidth 256
R1(config-if)#ip ospf cost 9500
R1(config-if)#
```

Configurar OSPFv2 en R2.

```
R2(config)#router ospf 1
R2(config-router)#router-id 5.5.5.5
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#
01:04:42: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from
LOADING to FULL, Loading Done

R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#int s0/0/1
R2(config-if)#bandwidth 256
R2(config-if)#ip ospf cost 9500
R2(config-if)#int s0/0/0
R2(config-if)#bandwidth 256
R2(config-if)#router ospf 1
R2(config-router)#passive-interface f0/0
R2(config-router)#passive-interface f0/1
R2(config-router)#do wr
Building configuration...
[OK]
```

Configurar OSPFv2 en R3.

```
R3(config)#router ospf 1
R3(config-router)#router-id 8.8.8.8
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
01:35:57: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/1/0 from
LOADING to FULL, Loading Done
```

```
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#auto-cost reference-bandwidth 9500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R3(config-router)#exit
R3(config)#int s0/1/0
R3(config-if)#bandwidth 256
R3(config-if)#exit
R3(config)#do wr
Building configuration...
[OK]
R3(config)#
```

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
En R2.

```
R2#show ip ospf neig
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
1.1.1.1	0	FULL/ -	00:00:33	172.31.21.1
Serial0/0/1				
8.8.8.8	0	FULL/ -	00:00:34	172.31.23.2
Serial0/0/0				

```
R2#
```

En R1.

```
R1#show ip ospf neig
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
5.5.5.5	0	FULL/ -	00:00:32	172.31.21.2
Serial0/1/0				
R1#				

En R3.

```
R3#show ip ospf neig
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
5.5.5.5	0	FULL/ -	00:00:38	172.31.23.1
Serial0/1/0				
R3#				

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface

```
[OK]
R2#show ip ospf interface

FastEthernet0/1 is up, line protocol is up
  Internet address is 10.10.10.1/24, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 5.5.5.5, Interface address 10.10.10.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 390
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 8.8.8.8
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
R2#
```

- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

R2.

```
router ospf 1
  router-id 5.5.5.5
  log-adjacency-changes
  passive-interface FastEthernet0/0
  passive-interface FastEthernet0/1
  network 172.31.21.0 0.0.0.3 area 0
  network 172.31.23.0 0.0.0.3 area 0
  network 10.10.10.0 0.0.0.255 area 0
!
```

R1.

```
router ospf 1
  router-id 1.1.1.1
  log-adjacency-changes
  passive-interface GigabitEthernet0/0
  passive-interface GigabitEthernet0/0.30
  passive-interface GigabitEthernet0/0.200
  passive-interface GigabitEthernet0/0.40
  auto-cost reference-bandwidth 9500
  network 172.31.21.0 0.0.0.3 area 0
  network 192.168.30.0 0.0.0.3 area 0
  network 192.168.40.0 0.0.0.3 area 0
  network 192.168.30.0 0.0.0.255 area 0
  network 192.168.40.0 0.0.0.255 area 0
  network 192.168.200.0 0.0.0.255 area 0
!
```

R3.

```
router ospf 1
  router-id 8.8.8.8
  log-adjacency-changes
  passive-interface Loopback4
  passive-interface Loopback5
  passive-interface Loopback6
  auto-cost reference-bandwidth 9500
  network 172.31.23.0 0.0.0.3 area 0
  network 192.168.4.0 0.0.3.255 area 0
!
```

2.3 Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Configurar vlan e interfaces en S1.

```
S1#config t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
S1(config)#do wr
Building configuration...
[OK]
S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
```

```
S1(config-if)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#do wr
Building configuration...
[OK]
S1(config-if)#int f0/1
S1(config-if)#switch mode access
S1(config-if)#switch access vlan 30
S1(config-if)#int range f0/2,f0/4-23, g0/1-2
S1(config-if-range)#shut
```

Configurar vlan e interfaces en S3.

```
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#int vlan 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to
up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#do wr
Building configuration...
[OK]
S3(config-if)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#
S3(config-if-range)#int f0/1
S3(config-if)#switch mode access
S3(config-if)#switch access vlan 40
```


Configurar vlan y sub-interfaces en R1.

```
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/0
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#
R1(config-if)#int g0/0.30
R1(config-subif)#
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/0.40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0

R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#int g0/0.200
R1(config-subif)#
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#do wr
Building configuration...
[OK]
```

2.4 En el Switch 3 deshabilitar DNS lookup

```
S3#config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
```

2.5 Asignar direcciones IP a los Switches acorde a los lineamientos.

Asignar ip S1.

```
S1(config)#int vlan 200
S1(config-if)#
S1(config-if)#ip address 192.168.99.2 255.255.255.0
```

```
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
```

Asignar ip S3.

```
S3(config)#int vlan 200
S3(config-if)#
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
```

2.6 Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Desactivar interfaces S1.

```
S1(config-if)#int range f0/2,f0/4-23, g0/1-2
S1(config-if-range)#shut
```

Desactivar interfaces S3.

```
S3# config t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#
S3(config)#int range f0/2, f0/4-24, g0/1-2
S3(config-if-range)#shut
```

2.7 Implement DHCP and NAT for IPv4

2.8 Configurar R1 como servidor DHCP para las VLANs 30 y 40.

2.9 Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

```
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
```

```
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool admin
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool merca
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#do wr
```

2.10 Configurar NAT en R2 para permitir que los hosts puedan salir a internet.

Debemos configurar R2 con NAT para permitir que los terminales A y C, puedan salir a internet.

```
R2(config)#user webserver privilege 15 secret cisco
R2(config)#do wr
Building configuration...
[OK]
R2(config)#ip http server
^
% Invalid input detected at '^' marker.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
R2(config)#
```

Nota: Debido a que packet tracer no soporto los comandos http y http server, se anexa un servidor a la topología.

Configuramos R2 con NAT.

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#do wr
Building configuration...
[OK]
```

- 2.11 Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#do wr
Building configuration...
[OK]
R2(config)#ip access-list standard ADMIN_S
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN_S in
R2(config-line)#do wr
Building configuration...
[OK]
R2(config-line)#
```

- 2.12 Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

```
R2(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
R2(config)#access-list 101 permit icmp any any echo-reply
R2(config)#int s0/0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#int s0/0/0
R2(config-if)#ip access-group 101 out
R2(config-if)#int f0/0
R2(config-if)#ip access-group 101 in
R2(config-if)#int f0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#do wr
Building configuration...
[OK]
```

2.13 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

```
R2#ping 209.165.200.230
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
R2#
```

```
R2#ping 10.10.10.10
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

```
R2#
```

```
R2#
```

```
R2#ping 172.31.23.2
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
```

```
R2#
```

```
R2#ping 172.31.21.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.31.21.1, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/13 ms
```

```
R2#
```

Traceroute.

```
R2#traceroute 172.31.21.1
Type escape sequence to abort.
Tracing the route to 172.31.21.1

 1  172.31.21.1      5 msec    0 msec    0 msec
R2#
```

```
R2#traceroute 172.31.23.2
Type escape sequence to abort.
Tracing the route to 172.31.23.2

 1  172.31.23.2      5 msec    1 msec    0 msec
R2#
```

```
R2#traceroute 10.10.10.10
Type escape sequence to abort.
Tracing the route to 10.10.10.10

 1  10.10.10.10      0 msec    0 msec    0 msec
R2#
```

Conclusiones.

En el presente trabajo se realizó la revisión de dos escenarios, donde se pide generar soluciones mediante los temas tratados en los cursos CCNA1 Y 2, en estas actividades se realizó la configuración de los protocolos RIPv2 y OSPFv2. La finalidad de los ejercicios fue lograr la interconexión de redes a través de protocolos de enrutamiento muy conocidos, permitiendo de esta forma obtener acceso a internet y a las diferentes redes conectadas de forma local y remota. Fue necesaria la utilización de protocolos de configuración como NAT, DHCPv4 y v6, ACL entre otros, de igual forma se realizó direccionamiento ip mediante el uso de VLAN para administración de cada uno de los segmentos de red y acceso a la web, en este proceso se permitió de igual forma la dinámica de configuración básica de dispositivos de red switches y routers, documentados mediante pantallazos con la utilización de comandos básicos como PING, TRACEROUTE, SHOW IP ROUTE.

Referencias bibliográficas.

Temática: Enrutamiento Dinámico

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

Temática: OSPF de una sola área

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

Temática: Listas de control de acceso

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

Temática: DHCP

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

Temática: Traducción de direcciones IP para IPv4

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>

OVA Unidad 4 - Video - Principios de Enrutamiento

Este Objeto Virtual de Aprendizaje, titulado Video - Principios de Enrutamiento, tiene como objetivo, orientar al estudiante sobre la configuración básica de Switches y Routers.

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgOyjWVeh6timi_Tm